



September 30, 2011

BY EMAIL

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Re: Docket No. R-1404 (RIN No. 7100 AD 63) - Debit Card Interchange Fees
and Routing

Dear Ms. Johnson:

Amazon.com, Inc. ("Amazon") respectfully submits the following comments concerning the interim final rule that the Board of Governors of the Federal Reserve System (the "Board") issued pursuant to Section 920 of the Electronic Fund Transfer Act (the "Act") concerning the fraud prevention adjustment. *See Debit Card Interchange Fees and Routing*, 76 Fed. Reg. 43,478 (proposed Jul. 20, 2011) ("Interim Final Rule").

Amazon appreciates the Board's diligent work as reflected in the Interim Final Rule and applauds the Board's decision to propose fraud prevention rules that are technologically neutral. However, we believe that the final rule ultimately adopted by the Board also:

- Must, as required by the Act, require that the fees paid by merchants to compensate for the cost of fraud prevention incurred by issuers correspond to cost-effective reduction in fraud;
- Must, as required by the Act, take into account merchants' fraud prevention costs; and
- Should include an independent, effective method for certifying issuer compliance with the Board's standards.

A. The final rule ultimately adopted by the Board must, as required by the Act, require that the fees paid by merchants to compensate for the cost of fraud prevention incurred by issuers correspond to cost-effective reduction in fraud.

According to the Act, the Board may permit a fraud prevention adjustment to the base interchange rate if one is "reasonably necessary to make allowance for costs incurred by

the issuer in preventing fraud.” Section 920(a)(5)(A)(i). Additionally, the statute requires any covered fraud prevention to be “cost effective” in order to qualify for an adjustment. *See* Section 920(a)(5)(A)(ii)(II) (Standards must “require issuers to take effective steps to reduce the occurrence of, and costs from, fraud in relation to electronic debit transactions, including through the development and implementation of cost-effective fraud prevention technology.”).

Respectfully, we believe that the Interim Final Rule incorrectly concludes that “[t]he phrasing ‘reasonably necessary to make allowance for’ fraud prevention costs does not require a direct connection between the fraud-prevention adjustment and actual issuer costs.” *See* 76 Fed. Reg. at 43482 (Section V.B.2 (Interim Final Rule)). While we agree that this language does not require a penny-for-penny match between the fraud adjustment and actual monies expended by an issuer, it certainly does contemplate a direct connection between the fraud prevention adjustment and actual issuer costs. To not require issuers to demonstrate the effectiveness of their fraud prevention measures and to show that those measures are actually cost-effective is inconsistent with the Act.

Industry commentators have concluded that virtually all, if not all, covered issuers can already certify compliance with the standards set forth in the Interim Final Rule without making any changes to their systems.

All debit card issuers have rudimentary fraud-prevention practices in place through their [Payment Card Industry Data Security Standard] requirements and card-network participation, so there is no reason to believe any issuer won’t qualify for the one-cent adjustment.

Statement of Beth Robertson, Director of Payments Research for Javelin Strategy & Research (Kate Fitzgerald, “Fed’s Fraud Allowance May Not Cover Debit Issuers’ Costs,” *American Banker*, Aug. 1, 2011).

The fact that even “rudimentary” systems can qualify for the adjustment indicates that the standards in the Interim Final Rule do not reflect the Act’s goal that issuers have an appropriate incentive to reduce fraud. Indeed, the fact that issuers can apparently qualify via the Payment Card Industry Data Security Standards (PCI DSS) highlights the problem. PCI DSS requirements are designed to protect customer data from theft and/or breach; in other words, they are *security* standards, not fraud standards. Even the issuers and merchants with the very best security will still experience fraud. The Act is intended to incent issuers to prevent fraud and to allow them to be compensated for this, so long as their investments are cost-effective. Issuers should not be able point to existing standards like PCI DSS security practices to qualify for the fraud adjustment when those standards do not prevent most forms of fraud. And if issuers are not required to demonstrate that their fraud prevention measures are cost-effective, merchants will be in the position of subsidizing ineffective fraud prevention measures, and the issuers will therefore have less of an incentive to improve the effectiveness of those programs.

We are also concerned that the requirements included in the Interim Final Rule are too vague and, thus, may inadvertently lead issuers to adopt policies and procedures that are inconsistent with providing an “economical means” for reducing fraud. Section 920(a)(5)(B)(ii)(III); *see also* 76 Fed. Reg. at 43478. For example, the guidelines suggest that issuers may qualify by using “dynamic data” to better authenticate a cardholder at the point-of-sale. 76 Fed. Reg. at 43487 (Section 235.4 Fraud-Prevention Adjustment, 4(b) Issuer Standards – Paragraph 4(b)(1)(i) at 1.iii). Such an approach could theoretically include existing cardholder authentication technologies like 3D Secure (commonly branded as Verified by Visa or MasterCard’s SecureCode), which has been found to be neither effective nor economical.

Some of the critiques of Verified by Visa and MasterCard’s SecureCode highlight the deficiencies inherent in an approach that mechanically rewards issuers for implementing such systems. The criticisms include that these systems, in effect, encourage shoppers to adopt risky security habits and, therefore, abet fraud rather than reduce it.¹ These systems are also prone to phishing attacks and, once they are compromised, make it easier for fraudsters to complete transactions.² The well-known Zeus Trojan specifically targeted this weakness of the 3-D Secure protocol in 2010 by displaying a fake “Verified by Visa” or MasterCard SecureCode enrollment screen to lure victims to give criminals financial information to execute unauthorized funds transfers.³ Finally, these authentication methods can be economically ineffective because they cause legitimate customers to abandon their transactions in numbers far greater than any fraud prevention benefit.⁴ Given that these systems actually introduce new risks into the system and can cause more harm than they prevent, we believe that fraud prevention standards faithful to the Act must not reward issuers for putting those systems or any similar systems in place.

We continue to believe that the best way to address all of the statutory requirements and assure consumers and retailers that the fraud prevention costs covered by the adjustment both prevent fraud and are cost-effective is to adopt a market-based solution. Let issuers deploy technologies and offer them to merchants based on their ability to reduce fraud while preserving legitimate sales. Merchants could determine for themselves which solutions sufficiently reduce fraud in a cost-effective manner and then decide which issuers’ solutions to purchase.

¹ *See, e.g.*, Tom Espiner, “Cambridge researchers knock Verified by Visa,” *ZDNet UK*, Jan. 27, 2010. Available at <http://www.zdnet.co.uk/news/security-threats/2010/01/27/cambridge-researchers-knock-verified-by-visa-40008732/>. The article discusses research from Steven J. Murdoch & Ross Anderson, “Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication,” *Computer Laboratory, University of Cambridge, UK*, Jan. 2010, available at <http://www.cl.cam.ac.uk/~rja14/Papers/fc10vbysecurecode.pdf>.

² *See* John Leyden, “Merchants and punters cry foul over Verified by Visa,” *The Register*, Oct. 23, 2008. Available at http://www.theregister.co.uk/2008/10/23/vbyv_analysis/.

³ Available at http://www.networkworld.com/news/2010/071310-zues-mastercard.html?source=www_rss.

⁴ Merchant implementations of these cardholder authentication practices have resulted in abandonment rates ranging from 6% to 60% as reported in studies found in public searches. Even if the true abandonment rate is closer to the minimal 6%, that still is far greater than the fraud rates experienced by most merchants.

Amazon believes that a truly market-based system (*i.e.*, not imposed under direct or indirect cover of network rules) will satisfy the core requirements of the Act, because only cost-effective technologies, from the standpoint of issuers and merchants, should qualify. This approach would stimulate issuer competition and avoid putting the Board in the position of constantly policing standards regarding the adequacy of various fraud prevention measures. If the Board determines not to adopt a market-based approach, we endorse the Board's imposition of a cap on any adjustment for issuer fraud prevention measures. A cap at least limits the negative impact on merchants that will result if issuers are not required to prove the effectiveness of their fraud prevention measures.

B. The final rule ultimately adopted by the Board must, as required by the Act, take into account merchants' fraud protection costs.

Under the Act, any fraud prevention adjustment set by the Board must account for merchants' fraud and fraud prevention costs. *See* Section 920(a)(5)(A)(ii)(I) ("standards shall ... take[] into account any fraud-related reimbursements (including amounts from charge-backs) received from ... merchants"); *see also* Section 920(a)(5)(B)(ii)(IV) (in crafting a fraud prevention standard, the Board "shall consider ... the fraud prevention and data security costs expended by each party involved in electronic debit transactions (including ... retailers)").

Despite these clear requirements to consider retailers' costs, the Interim Final Rule is based solely on the fraud prevention costs reported by certain issuers reported in the issuer survey. *See* 76 Fed. Reg. at 43482-83 (Section V.B.2 (Section 235.4(a) Adjustment Amount – Interim Final Rule)) (calculating 1-cent adjustment by deducting 0.7 cents from median issuers' 1.8 cent costs as reported in survey). Numerous comments in the initial proceeding, including those submitted by Amazon, describe the significant fraud prevention costs borne by merchants, including fraud, fraud prevention, and data security costs. Basically, and contrary to the requirements of the Act, merchant costs were never surveyed by the Board and are simply not accounted for in the Interim Final Rule.

Like banks and credit card brands, merchants employ a variety of means to prevent fraud and mitigate risk. The extent and sophistication of these means vary by merchant according to their size, environment, and capabilities, but almost all merchants have adopted means to reduce their fraud risk, including with internally developed or commercially purchased technology systems. The failure to account for the costs incurred by merchants cannot be reconciled with the Act and calls into question whether the \$.01 per transaction fraud adjustment is justified.

The treatment of merchants with card-not-present transactions highlights this concern. As we explained in our previous letter to the Board, merchants bear the entire cost of fraud losses on card-not-present transactions. As a result, a merchant like Amazon must invest significantly in fraud prevention measures of its own in order to minimize fraud losses. If the costs incurred by Amazon in preventing fraud are not considered, an issuer

can charge the same fraud adjustment to Amazon that it charges to a merchant that is not responsible for fraud losses. In other words, by not considering merchants' costs, as required by the Act, merchants like Amazon would subsidize the fraud prevention for the rest of the network. The final rule ultimately adopted by the Board must take into account these costs.

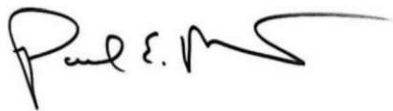
Once again, these concerns would not be present in a performance-based approach to the fraud adjustment. Issuers would deploy fraud prevention technologies that take into account the costs of those measures and merchants would choose to accept or reject them based on their own costs (including the fraud prevention adjustment and the costs incurred separately by the merchant in preventing fraud) like they currently do with other commercially available fraud prevention services. In that way, our proposed solution would reflect the costs of both and therefore comply with the Act.

C. The final rule ultimately adopted by the Board should include an independent, effective method for certifying issuer compliance with the Board's standards.

The Interim Final Rule would require that issuers certify compliance with the Board's fraud prevention adjustment standards to their payment network providers. Should the Board maintain this approach, we respectfully suggest that the responsibility for overseeing issuer compliance not be given to the networks, because they have an interest in minimizing burdens on issuers to attract their business. In order to avoid any conflict of interest, certification of compliance with the fraud adjustment requirements should be done by the Board itself or a competent, disinterested third party designated and overseen by the Board.

Thank you in advance for your attention to the comments in this letter. Please let me know if you have any questions. I may be reached at pmisener@amazon.com or 202-347-7390.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Paul E. Misener", with a stylized flourish at the end.

Paul Misener
Vice President for Global Public Policy